ОКРУЖНОЙ СУД США
ПО ВОСТОЧНОМУ ОКРУГУ ШТАТА ВИРДЖИНИЯ
Александрийское отделение

КОРПОРАЦИЯ «МАЙКРОСОФТ», зарегистрированная в штате Вашингтон, и фирма FS-ISAC, INC., зарегистрированная в штате Делавер, истцы, против НЕИЗВЕСТНЫХ ЛИЦ 1-8 1-8, КОНТРОЛИРУЮЩИХ КОМПЬЮТЕРНУЮ БОТ-СЕТЬ, ЧТО НАНОСИТ УЩЕРБ КОМПАНИИ МАЙКРОСОФТ И ЕЕ КЛИЕНТАМ, ответчики.	)	Гражданский иск №: **ПОДАН СОГЛАСНО ПРОЦЕДУРАМ КОНФИДЕНЦИАЛЬНОСТИ**

ИСК

Истцы КОРПОАРЦИЯ МАЙКРОСОФТ («Майкрософт») и фирма FS-ISAC, INC., (“FS-ISAC”), подавая настоящий иск, обвиняют неизвестных лиц 1-8 (коллективно - «Истцы») в том, что они контролируют глобальную сеть взаимосвязанных противозаконных компьютерных сетей, известную под коллективным названием «бот-сети Шейлока», состоящую из компьютеров пользователей, подсоединенных к интернету, которые истцы заразили вредоносным программным обеспечением. Истцы использовали бот-сети Шейлока для заражения подключенных к интернету компьютеров, а затем использовали их для хищения многих миллионов долларов. Истцы контролируют бот-сети Шейлока с помощью сложной командно-контрольной инфраструктуры, размещенной в доменах интернета («домены») и серверах доменных имен, перечисленных в приложении А к настоящему иску, и управляемой через их посредство. («домены Шейлока»), IP-адресов, перечисленных в приложении В к настоящему иску ("IP-адреса Шейлока") (коллективно – «командно-контрольная инфраструктура Шейлока»). Истцы

утверждают следующее:

ХАРАКТЕР ИСКА

1. Настоящий иск основан на следующих правовых нормах: (1) закон «О компьютерном мошенничестве и злоупотреблениях», 18 U.S.C. § 1030; (2) закон «Об охране личной информации при использовании электронных средств связи», 18 U.S.C. § 2701; (3) закон Ланхэма в части нарушения правил использования торговых марок, 15 U.S.C. § 1114 et seq. (4) закон Ланхэма в части ложного указания происхождения, 15 U.S.C. § 1125(a); (5) закон Ланхэма в части несанкционированного использования торговых марок, 15 U.S.C. § 1125(c); (6) закон «О вымогательстве и преступных организациях», (18 U.S.C. § 1962(c)); (7) положения прецедентного права о незаконном пользовании движимой собственностью; (8) положения о противоправном обогащении и (9) положения о незаконном присвоении имущества. Истцы просят о выпуске судебных распоряжений и других равносильных мерах, а также требуют компенсации ущерба со стороны истцов, управляющих контролируемыми компьютерными сетями – т.е. «бот-сетями Шейлока» - через командно-контрольную инфраструктуру Шейлока. Используя бот-сети Шейлока, истцы нанесли и продолжают наносить невосполнимый ущерб истцам, входящим в их состав структурам, их клиентам и обществу.

СТОРОНЫ

2. Истец «Майкрософт» является корпорацией, надлежащим образом организованной и существующей по законам штата Вашингтон. Ее штаб-квартира и основное место осуществления деловой деятельности расположены в г. Редмонд, Вашингтон.

3. Истец FS-ISAC, Inc. является некоммерческой корпорацией, надлежащим образом организованной и существующей по законам штата Делавер. Ее штаб-квартира и основное место осуществления деловой деятельности расположены в г. Рестон, Виргиния. FS-ISAC является объединением, состоящим из 4400 организаций-членов, включая коммерческие банки и кредитные союзы всех размеров, брокерские фирмы, страховые компании, процессинговые фирмы, а также более 20 торговых ассоциаций,

представляющих бóльшую часть сектора финансовых услуг США. FS-ISAC представляет интересы своих членов, предоставляющих финансовые услуги, в борьбе с кибер-угрозами и защите от них, поскольку означенные угрозы чреваты риском и убытки для данной отрасли.

4. Имеющаяся информация позволяет прийти к заключению, что **неизвестное лицо 1** контролирует бот-сеть Шейлока, идентифицированную как бот-сеть “USA” с целью осуществления действий, предназначенных для нанесения ущерба истцам, их клиентам и обществу. На основе полученной информации истцы пришли к выводу, что с неизвестным лицом 1, по всей видимости, можно связаться непосредственно или через третьи стороны при помощи данных, приведенных в приложениях A и B.

5. Имеющаяся информация позволяет прийти к заключению, что **неизвестное лицо 2** контролирует бот-сеть Шейлока, идентифицированную как бот-сеть “HJ-UK-1” с целью осуществления действий, предназначенных для нанесения ущерба истцам, их клиентам и обществу. На основе полученной информации истцы пришли к выводу, что с неизвестным лицом 2, по всей видимости, можно связаться непосредственно или через третьи стороны при помощи данных, приведенных в приложениях A и B.

6. Имеющаяся информация позволяет прийти к заключению, что **неизвестное лицо 3** контролирует бот-сеть Шейлока, идентифицированную как бот-сеть “HJ-UK-2” с целью осуществления действий, предназначенных для нанесения ущерба истцам, их клиентам и обществу. На основе полученной информации истцы пришли к выводу, что с неизвестным лицом 3, по всей видимости, можно связаться непосредственно или через третьи стороны при помощи данных, приведенных в приложениях A и B.

7. Имеющаяся информация позволяет прийти к заключению, что **неизвестное лицо 4** контролирует бот-сеть Шейлока, идентифицированную как бот-сеть “HJ-UK-3” с целью осуществления действий, предназначенных для нанесения ущерба истцам, их клиентам и обществу. На основе полученной информации истцы пришли к выводу, что с неизвестным лицом 4, по всей видимости, можно связаться непосредственно или через третьи стороны при помощи данных, приведенных в приложениях A и B.

8. Имеющаяся информация позволяет прийти к заключению, что **неизвестное лицо 5** контролирует бот-сеть Шейлока, идентифицированную как бот-сеть “HJ-UK-4” с целью осуществления действий, предназначенных для нанесения ущерба истцам, их клиентам и обществу. На основе полученной информации истцы пришли к выводу, что с неизвестным лицом 5, по всей видимости, можно связаться непосредственно или через третьи стороны при помощи данных, приведенных в приложениях A и B.

9. Имеющаяся информация позволяет прийти к заключению, что **неизвестное лицо 6** контролирует бот-сеть Шейлока, идентифицированную как бот-сеть “net1” с целью осуществления действий, предназначенных для нанесения ущерба истцам, их клиентам и обществу. На основе полученной информации истцы пришли к выводу, что с неизвестным лицом 6, по всей видимости, можно связаться непосредственно или через третьи стороны при помощи данных, приведенных в приложениях A и B.

10. Имеющаяся информация позволяет прийти к заключению, что **неизвестное лицо 7** контролирует бот-сеть Шейлока, идентифицированную как бот-сеть “net2” с целью осуществления действий, предназначенных для нанесения ущерба истцам, их клиентам и обществу. На основе полученной информации истцы пришли к выводу, что с неизвестным лицом 7, по всей видимости, можно связаться непосредственно или через третьи стороны при помощи данных, приведенных в приложениях A и B.

11. Имеющаяся информация позволяет прийти к заключению, что **неизвестное лицо 8** контролирует бот-сеть Шейлока, идентифицированную как бот-сеть “net3” с целью осуществления действий, предназначенных для нанесения ущерба истцам, их клиентам и обществу. На основе полученной информации истцы пришли к выводу, что с неизвестным лицом 8, по всей видимости, можно связаться непосредственно или через третьи стороны при помощи данных, приведенных в приложениях A и B.

12. Третьи стороны VeriSign Naming Services и VeriSign Global Registry Services (коллективно - “VeriSign”) являются реестрами доменных имен, осуществляющими надзор над регистрацией всех доменных имен, заканчивающихся на “.net,” “.cc,” и “.com.” Фирма VeriSign Name Services расположена по адресу 21345 Ridgetop Circle, 4th Floor,

Dulles, Virginia 20166. Фирма VeriSign Global Registry Services расположена по адресу 12061 Bluemont Way, Reston, Virginia 20190.

13. В приложениях A и B приводятся наименования и контактная информация для третьих сторон – реестров доменных имен, контролирующих домены, используемые ответчиками, а также для третьих сторон – хостинговых компаний, контролирующих серверы, используемые ответчиками.

14. Имеющаяся информация позволяет прийти к заключению, что неизвестные лица 1-8 совместно владеют, контролируют, поддерживают и осуществляют свою деятельность под именами бот-сети Шейлока и Командно-контрольная инфраструктура Шейлока. Истцы внесут в данный иск поправки, указав настоящие имена и функции ответчиков, когда они будут установлены. Истцы приложат надлежащие усилия с целью определения истинных имен, функций и контактной информации неизвестных лиц 1-8 и доставки им материалов данного судебного дела.

15. Согласно полученной информации, истцы пришли к заключению, что каждый из неизвестных лиц-ответчиков в той или мере несет ответственность за действия, в которых они обвиняются в данном иске, и что в соответствующем нанесении ущерба истцам непосредственно виновны данные ответчики.

16. Имеющаяся информация позволяет прийти к заключению, что действие и бездействие, в которых обвиняются неизвестные лица 1-8, представляли собой действия, которые каждый из ответчиков утверждал, контролировал, направлял, или имел возможность утверждать, контролировать или направлять, и/или представляли собой действия и бездействие, в которых каждый из ответчиков осуществлял помощь, участвовал или иным образом поощрял, и являются действиями, за которые несет ответственность каждый из ответчиков. Каждый из ответчиков способствовал осуществлению описанных ниже действий, поскольку каждый ответчик знал об этих действиях или бездействии, предоставлял помощь и получал выгоду от этих действий и бездействия полностью или частично. Каждый ответчик представлял собой агента всех остальных ответчиков и, осуществляя деятельность, в которой он обвиняется ниже,

действовал в соответствии с направлением и масштабами своих агентских услуг и с согласия и разрешения остальных ответчиков.

ЮРИСДИКЦИЯ И МЕСТО СУДЕБНЫХ СЛУШАНИЙ

17. Настоящий суд обладает существенной юрисдикцией по данному делу в соответствии с 28 U.S.C. § 1331, поскольку настоящий иск вызван нарушениями со стороны ответчиков таких правовых норм, как федеральный закон «О компьютерном мошенничестве и злоупотреблениях» (18 U.S.C. § 1030), закон «О контроле над электронным распространением порнографии и маркетингом» (15 U.S.C. § 7704), закон «Об охране личной информации при использовании электронных средств связи» (18 U.S.C. § 2701); закон «О вымогательстве и преступных организациях» (18 U.S.C. § 1962(c)); а также закон Ланхэма (15 U.S.C. §§ 1114, 1125). Суд обладает также существенной юрисдикцией в части жалобы истцов на незаконное пользование имуществом, противоправное обогащение и противозаконное присвоение имущества в соответствии с 28 U.S.C. § 1367.

18. Имеющаяся информация позволяет прийти к заключению, что выбор места слушаний в данном судебном округе в соответствии с 28 U.S.C. § 1391(b) проведен обоснованно, поскольку значительная часть событий или бездействия, вызвавших появления настоящего иска, имела место в данном судебном округе, где располагается также значительная доля собственности, являющейся предметом иска со стороны ответчиков. Ответчики располагают компьютерами и веб-сайтами, а также осуществляют иные действия, позволяющие им вести бизнес в Виргинии, и с помощью технических средств, расположенных в Виргинии и Восточном округе Виргинии, осуществляют действия, являющиеся предметом жалобы Истца.

19. Ответчики прямо направляют свои действия на Виргинию и Восточный округ Виргинии, рассылая вредоносные компьютерные коды на компьютеры индивидуальных пользователей, расположенных в Виргинии и Восточном округе Виргинии, стремясь заразить эти пользовательские компьютеры вредоносным кодом и включить эти пользовательские компьютеры в “бот-сеть”, которая используется для

нанесения ущерба Истцам, их клиентам и обществу в целом. На следующих иллюстрациях отражено географическое расположение пользовательских компьютеров в Виргинии (**Рис. 1**) и Восточном округе Виргинии (**Рис. 2**), на которые Ответчики заведомо рассылали вредоносный код, стремясь заразить данные компьютеры и включить их в бот-сеть:

Рис. 1

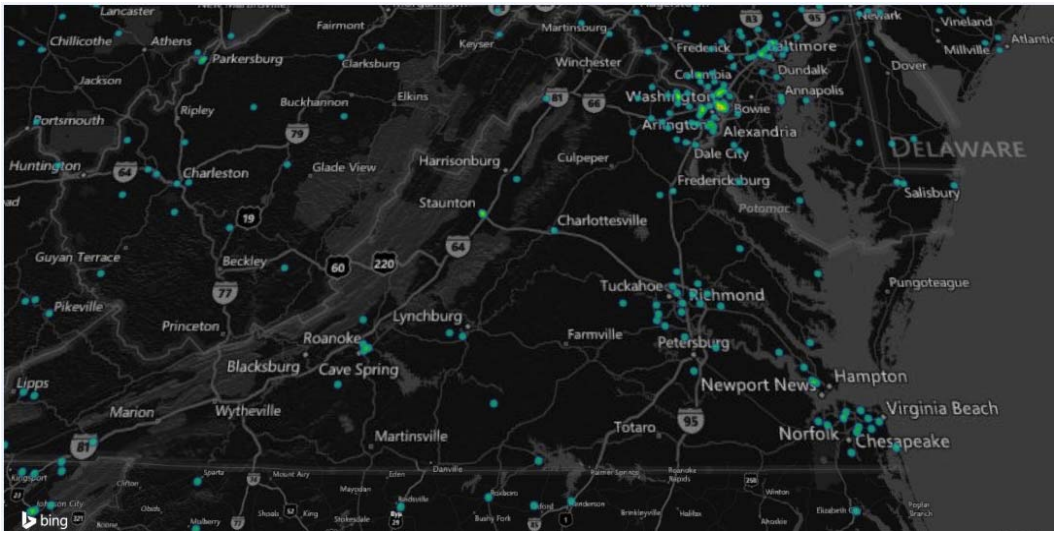
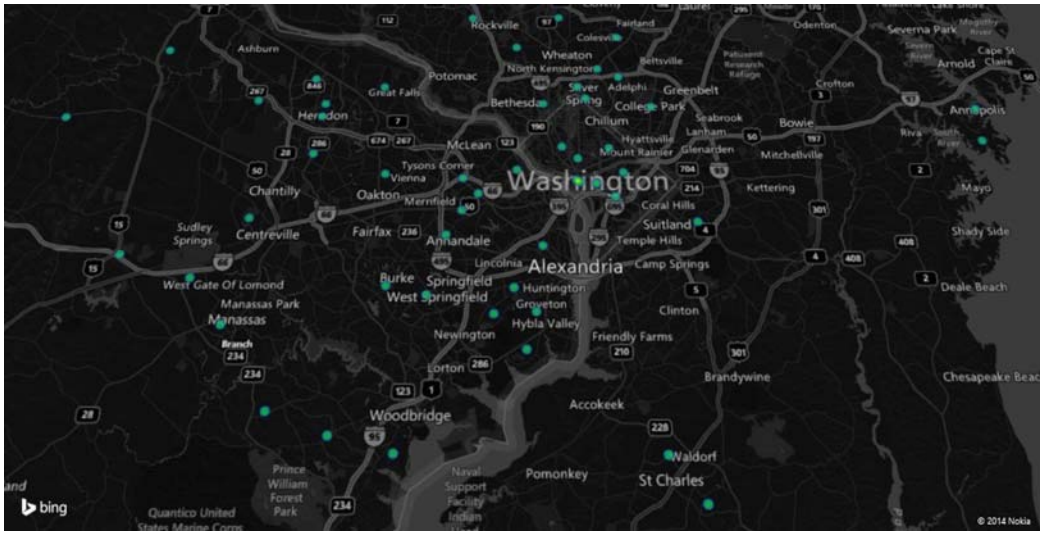


Рис. 2



20. Ответчики поддерживают ряд доменов Шейлока, зарегистрированных через VeriSign и Public Interest Registry, расположенных в Восточном округе Виргинии. Ответчики используют эти домены для контроля коммуникаций бот-сетей Шейлока,

принадлежащих, эксплуатируемых и поддерживаемых Ответчиками в данном юридическом округе. Ответчики совершали упоминаемые здесь действия, отдавая себе отчет в том, что данные действия нанесут ущерб посредством доменов, расположенных в Восточном округе Виргинии, посредством доменов Шейлока, поддерживаемых через объекты в Восточном округе Виргинии, и посредством пользовательских компьютеров, расположенных в Восточном округе Виргинии, таким образом причиняя ущерб Истцам, клиентам и члена организаций Истцов, а также другим лицам в Восточном округе Виргинии и в других частях Соединенных Штатов. На этом основании Ответчики подпадают под непосредственную юрисдикцию данного Суда.

21. В соответствии с 28. U.S.C. § 1391(b), территориальная подсудность имеет место в данном юридическом округе. Существенная часть событий или несовершенных действий, на которых основаны иски Истцов, а также существенная часть собственности, являющейся предметом исков Истцов, находятся в данном юридическом округе. Территориальная подсудность имеет место в данном юридическом округе согласно 28 U.S.C. § 1391(c), поскольку Ответчики подпадают под личную юрисдикцию в данном юридическом округе.

ФАКТИЧЕСКИЕ СВЕДЕНИЯ

Деятельность и репутация истцов

22. Microsoft® является провайдером операционной системы Windows® и браузера Internet Explorer®, а также ряда других программ и услуг. Microsoft инвестировал существенные средства в разработку качественных продуктов и услуг. Благодаря высокому качеству и эффективности продуктов и услуг Microsoft и затрате этой компанией значительных средств на маркетинг данных продуктов и услуг, компания приобрела существенную репутацию у клиентов, создав сильный бренд и превратив название компании Microsoft и названия ее продуктов и услуг в уважаемые и известные во всем мире символы, которые обладают высокой узнаваемостью в ее торговых сферах. Microsoft обладает зарегистрированными торговыми марками, отражающими качество продуктов и услуг этой компании и ее бренда, включая Microsoft®, Windows® и Internet

Explorer®. Копии регистрационных документов торговых марок Microsoft, Windows и Internet Explorer включены в Приложение C к настоящему Иску.

23. Истец FS-ISAC является торговой организацией, состоящей из 4400 организаций, включая коммерческие банки и кредитные союзы различных размеров, брокерские фирмы, страховые компании, платежные системы и более 20 торговых ассоциаций, представляющих большинство секторов финансовых услуг США. Она была учреждена сектором финансовых услуг в ответ на 63-й указ Президента от 1998 г., позднее обновленный 7-м указом Президента о национальной безопасности от 2003 г., который требует, чтобы государственный и частный секторы делились информацией об уязвимости и физических и кибер-угрозах безопасности с целью защиты критической инфраструктуры Соединенных Штатов. (См. www.fsisac.com/about/). Ее цель заключается в "укреплении способности сектора финансовых услуг подготовиться к кибер- и физическим угрозам, уязвимости и интересам и реагировать на них ...." Деятельность FS-ISAC включает активную координацию мер по обнаружению финансовым сектором кибер-угроз безопасности, анализа таких угроз и реагирования на них, и содействие таким мерам. FS-ISAC тесно сотрудничает с различными государственными учреждениями, включая Министерство финансов США, Министерство внутренней безопасности (DHS), Федеральную резервную систему, регулирующие органы Федерального Совета по надзору за финансовыми учреждениями, Секретную службу Соединенных Штатов, Федеральное бюро расследований, Агентство национальной безопасности, Центральное разведывательное управление, а также местные органы власти и органы власти штатов. Финансовые учреждения, которые являются членами FS-ISAC, обладают существенной репутацией у своих клиентов, превратив свои соответствующие названия и названия своих продуктов и услуг в уважаемые и известные во всем мире символы, которые обладают высокой узнаваемостью в их торговых сферах.

Компьютерные «бот-сети»

24. «Бот-сеть» - это совокупность отдельных компьютеров, зараженных вредоносными программами (ВПО), позволяющая этим компьютерам связываться друг с

другом, а также поддерживать централизованную или нецентрализованную связь с другими компьютерами для получения контрольных инструкций. Бот-сеть может состоять из большого числа (иногда доходящего до миллионов) зараженных пользовательских компьютеров. Индивидуальные компьютеры в такой сети нередко принадлежат пользователям, которые без своего ведома загрузили вредоносное ПО или оказались им заражены. Пользовательский компьютер может стать часть. бот-сети, например, когда ничего не подозревающий владелец взаимодействует с вредоносным рекламным объявлением на веб-сайте, открывает вредоносное приложение к электронному письму или скачивает вредоносное ПО. В каждом из этих случаев вредоносное ПО загружается или запускается на компьютере пользователя, после чего он становится частью бот-сети. Превратишись в часть бот-сети, компьютер получает возможность получать и рассылать сообщения, коды и инструкции от (или на) другие компьютеры бот-сети.

25. Некоторые компьютеры бот-сети полностью находятся под контролем создателей последней. Они могут осуществлять специальные функции, например, рассылать контрольные инструкции зараженным пользовательским компьютерам. Их обычно называют «командно-контрольными» компьютерами.

26. Преступные организации и индивидуальные киберпреступники часто создают, контролируют, поддерживают и распространяют бот-сети для совершения неправомерных действий, ущемляющих права других лиц. Они используют бот-сети из-за их способности поддерживать широкий круг незаконных действий, устойчивости к попыткам обезвреживания и способности скрывать личности контролирующих их правонарушителей. Лица, контролирующие бот-сеть, используют зараженный компьютер пользователя для реализации множества незаконных целей, о которых конечный пользователь не знает. Например, компьютер в бот-сети может использоваться для следующего:

a. кража учетных данных и информации, мошенничество, проникновение в компьютер или другие неправомерные действия;

b. анонимная рассылка объемных незапрашиваемых электронных

писем без ведома или согласия индивидуального пользователя, которому принадлежит взломанный компьютер;

c. дальнейшая рассылка вредоносных программ, заражающих другие компьютеры;

d. «проксирование» или ретрансляция сообщений в Интернете с других компьютеров с целью сокрытия истинного источника этих сообщений.

27. Бот-сети представляют собой очень эффективное средство контроля большого числа компьютеров и средство направления действия внутрь, против содержимого этих компьютеров, или вовне — против других компьютеров в Интернете.

Обзор бот-сетей Shylock

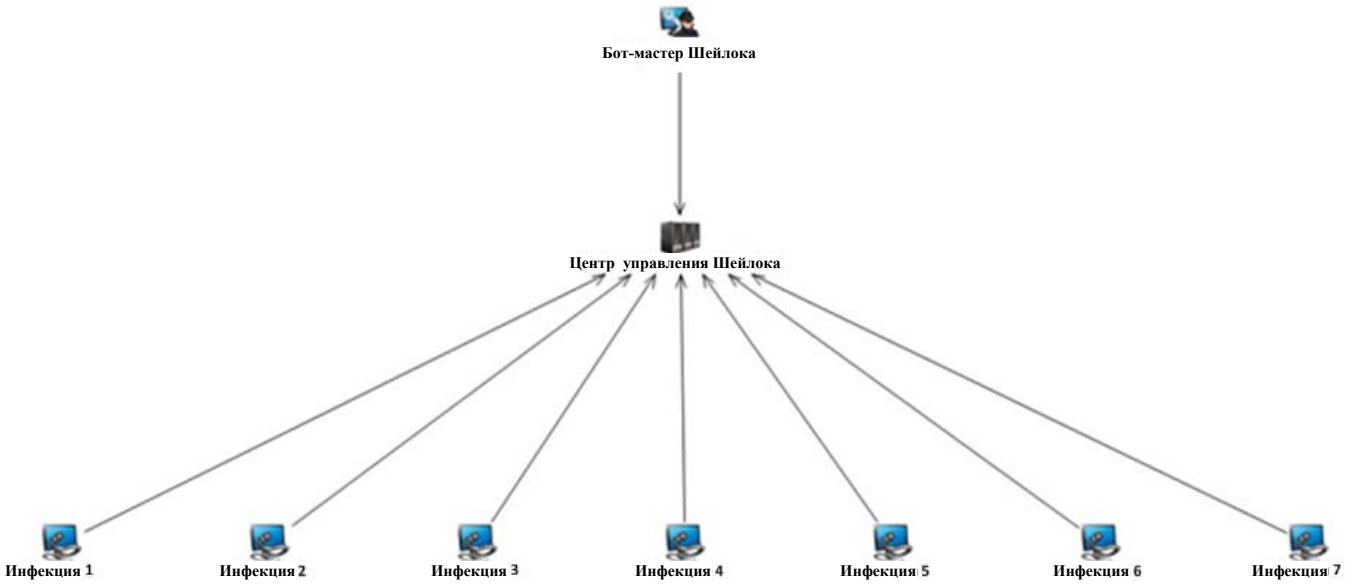
28. Истцы подают данный иск, чтобы прекратить причинение Ответчиками вреда Истцам, заказчикам и членам организаций Истцов, а также населению через командно-контрольную инфраструктуру Shylock, являющуюся центром для бот-сетей Shylock.

29. Ответчики используют бот-сети Shylock главным образом для получения доступа к данным учетных записей веб-сайтов дистанционного банковского обслуживания для кражи, помимо прочего, средств у пользователей компьютеров и у финансовых учреждений. Когда пользователь зараженного программами Shylock компьютера пытается войти на сайт финансового учреждения, Shylock: (a) скрытно вторгается в браузер пользователя; (b) считывает учетные данные пользователя для подключения к финансовому учреждению и другую персональную идентифицирующую информацию; (c) отправляет эту информацию Ответчикам. Пользователь не подозревает о деятельности Shylock, так как Ответчики разработали Shylock таким образом, чтобы скрывать самих себя и свою противоправную деятельность на зараженных компьютерах. После захвата сетью Shylock учетных данных пользователя для подключения к персональной идентифицирующей информации Ответчики используют эту информацию, например, для доступа к банковскому счету пользователя. Пользователь видит только

обычные учетные данные и не знает о том, что Ответчики ведут наблюдение, контролируют его компьютер и крадут данные о его личности и денежные средства с его счета.

Инфраструктура бот-сетей Shylock

30. Бот-сети Shylock имеют многоуровневую архитектуру, представленную ниже:



31. Самый нижний «**зараженный уровень**» в этой архитектуре, по оценкам, состоит из пользовательских компьютеров, зараженных Shylock. Это могут быть домашние стационарные компьютеры, ноутбуки или компьютеры в публичных библиотеках. Эти зараженные пользовательские компьютеры и являются по сути работниками бот-сетей Shylock, которые осуществляют повседневную незаконную деятельность, включая кражу учетных данных пользователей и заражение других пользовательских компьютеров.

32. Ответчики используют обманные методы для заражения других компьютеров. На основании сведений и предположений можно сделать вывод, что Ответчики, контролирующие бот-сети Shylock, является частью преступного предприятия,

иск

заразившего законные интернет-сайты и (или) создавшего интернет-сайты, специально рассчитанные на заражение пользовательских компьютеров. Когда ни о чем не подозревающий пользователь просматривает эти интернет-сайты, его компьютер перенаправляется на другой интернет-сайт, где загружается «пакет-эксплуататор», который скрытно зондирует компьютер пользователя в поиске уязвимых мест и возможностей выполнить код или установить вредоносную программу в систему.

33. После установки пакет-эксплуататор загружает и устанавливает вредоносную программу Shylock на пользовательский компьютер. Известно, что Ответчики заразили объявления в рекламной сети YouTube, чтобы перенаправлять пользователей на вредоносные веб-сайты. Ответчик также атаковал программы мгновенного обмена сообщениями, используя их для рассылки фальшивых сообщений другим пользователям об услугах мгновенного обмена в попытке перенаправить их на сайты-эксплуататоры. Кроме того, Ответчики снабдили Shylock средством удаленного доступа, что позволяет Ответчикам получать доступ к незараженным пользовательским компьютерам в зараженных Shylock локальных сетях. Эта функция по сути дает Ответчикам доступ через черный ход к незараженным пользовательским компьютерам, которые не являются частью бот-сетей Shylock.

34. Компьютеры, зараженные Shylock, используются Ответчиками в противоправной деятельности, включая (a) кражу учетных данных пользователей для дистанционного подключения к финансовым учреждениям и другим дистанционным учетным записям; (b) кражу персональной идентифицирующей информации пользователей; (c) кражу денежных средств у пользователей и финансовых учреждений; (d) взлом браузеров пользователей; (e) проверку компьютеров пользователей на наличие другой чувствительной информации, а также для другой незаконной деятельности. Большая часть владельцев зараженных Shylock компьютеров, если не все, не подозревают, что их компьютеры заражены и действуют как часть бот-сетей Shylock.

35. На самом высоком уровне архитектуры находится «**командно-контрольный уровень**», который состоит из доменов, серверов имен доменов и IP-

адресов, которые Ответчики используют и контролируют как командно-контрольные серверы для непрерывного контроля зараженных Shylock компьютеров. Термин «командно-контрольные серверы» относится либо к физическим компьютерам-серверам, либо к программному обеспечению, работающему на компьютерах, поддерживающих бот-сети Shylock. Число и местонахождение командно-контрольных серверов Shylock могут со временем изменяться.

Командно-контрольная инфраструктура Shylock

36. Командно-контрольная инфраструктура Shylock включает две группы ресурсов. Первая — домены Shylock, которые включают домены и имена серверов, используемые Ответчиками для связи с бот-сетью и ее расширения. «Жестко запрограммированные» домены Shylock содержат инструкции для зараженных Shylock компьютеров, включая exe-файлы «Шейлока», которые устанавливают вредоносную программу Shylock на пользовательские компьютеры. Жестко запрограммированные домены Shylock могут служить также резервными доменами на случай, если зараженный Shylock компьютер потеряет контакт с командно-контрольной инфраструктурой Shylock. Домены типа «конфигурационный файл» содержат конфигурационные файлы Shylock, которые загружают зараженные Shylock компьютеры. Конфигурационные файлы Shylock являются шифрованными текстовыми файлами, которые Ответчики используют для контроля зараженных компьютеров. Конфигурационные файлы включают, помимо прочего, команды, позволяющие Ответчиками совершать незаконные действия. Ответчики разработали Shylock таким образом, чтобы он мог адаптироваться через съемные модули, что позволяет Ответчикам снабжать центральный блок Shylock дополнительными функциями даже после установки Shylock. Эти съемные модули включают механизм, который используется Ответчиками для заражения программ мгновенного обмена сообщениями пользователя, и механизм удаленного доступа для доступа к незараженным пользовательским компьютерам и их атаки. Ответчики поддерживают также домены «носитель денег», которые он использует для привлечения «носителей денег» с целью сбора и перевода украденных денежных средств на счета

Ответчиков. Ответчики используют серверы имен доменов для хранения доменов, контролирующих бот-сети Shylock. В **Приложении А** к данному Иску перечислены домены Shylock.

37. Вторая группа — IP-адреса Shylock, которые Ответчики используют, чтобы хранить конфигурационные файлы и инструкции, необходимые для роста и поддержания бот-сетей Shylock. В **Приложении В** к данному Иску перечислены IP-адреса Shylock.

Ответчики используют бот-сети Shylock для кражи денег

38. Главная цель бот-сетей Shylock — это кража учетных финансовых данных владельцев зараженных Shylock компьютеров для доступа к их финансовым счетам и присвоения денежных средств Ответчиком. Ответчики через бот-сети Shylock использует несколько способов проведения таких атак.

39. Атака Shylock начинается, когда он обнаруживает попытку пользователя связаться с веб-сайтом финансового учреждения. Когда это происходит, Shylock может действовать несколькими способами. Например, он может отслеживать, какие клавиши пользователь нажимает при подключении к своей учетной записи. Shylock может использовать нажатия клавиш для доступа к финансовым учетным записям пользователя, записи информации пользователя, показанной на интернет-странице и даже делать скриншот или видеозапись страниц учетных записей пользователя. В последующем Shylock загружает эту информацию в свою командно-контрольную инфраструктуру. Ответчики могут использовать эту информацию для попытки украсть дополнительную информацию из учетной записи пользователя или предпринять другие незаконные действия с украденной информацией.

40. В более изощренном варианте этой базовой атаки вредоносное программное обеспечение бот-сетей Shylock, работающее на зараженных компьютерах, может предпринять атаку «закачка через сеть» для извлечения более чувствительной информации пользователя. При атаке «закачка через сеть» Shylock изменяет внешний вид интернет-страницы финансового учреждения, которая показывается в браузере пользователя. По сути Shylock устанавливает контроль над браузером пользователя.

Вместо того чтобы позволить браузеру точно отобразить интернет-страницу финансового учреждения, Shylock заставляет браузер изменить то, что видит пользователь. Он делает это путем «закачки» дополнительного кода в код веб-сайта, который браузер отображает в визуализируемом формате для пользователя. Например, если реальная интернет-страница запрашивает только имя и пароль для подключения, Shylock может расширить запрос путем «закачки через сеть» и запросить дополнительную информацию, например, номер социального страхования, дату рождения, девичью фамилию матери и другую подобную информацию, обычно используемую для вопросов, задаваемых в целях обеспечения безопасности. Shylock также записывает эту информацию и в последующем загружает ее Ответчикам, которые могут использовать ее для кражи у пользователя. Shylock способен использовать таким образом разные браузеры, включая Microsoft Internet Explorer и Mozilla Firefox.

41. В еще более изощренных версиях этой атаки Shylock может просто отобразить абсолютно подложный веб-сайт финансового учреждения, в которое пытается обратиться пользователь. Для этого злоумышленники сначала захватывают браузер, не давая ему подключиться к реальному веб-сайту финансового учреждения. Затем он подключается к командно-контрольной инфраструктуре Shylock и загружает шаблон веб-сайта финансового учреждения и отображает его на экране монитора пользователя. Пользователь, полагая, что подключился к реальному веб-сайту финансового учреждения, продолжает свои действия в обычном режиме. Однако когда пользователь вводит на подложном веб-сайте информацию для доступа к своему реальному счету, например, свой логин и пароль, Ответчики получают возможность доступа к счетам пользователя на реальном веб-сайте. Информация со счета на реальном веб-сайте может отображаться на экране монитора пользователя, зашедшего на поддельный веб-сайт, чтобы мошенники могли успешно завершить кражу. Для совершения кражи Ответчики могут изменить транзакции, осуществляемые на реальном веб-сайте, например, изменив суммы, снимаемые со счета и информацию о том, куда должны быть переведены деньги.

42. В некоторых случаях Ответчики заменяют только отдельные части веб-

сайта финансового учреждения. Например, Ответчики размещают номера телефонов Shylock на веб-сайте финансового учреждения. Истцы располагают информацией, убеждены и на этом основании утверждают, что Ответчики изменяют эти номера с целью предотвращения ситуаций, когда у пользователя возникают подозрения или он начинает замечать признаки мошенничества и пытается связаться с банком.

43. Ответчики постоянно злоупотребляют торговыми марками финансовых учреждений на этих поддельных банковских веб-сайтах с целью сбить с толку и ввести в заблуждение потерпевших. Что еще более важно, внедренная злоумышленниками информация содержит торговые марки учреждений-членов FS-ISAC. Ответчики разрабатывают свои подделки и используют торговые марки таким образом, чтобы как можно реалистичнее имитировать подлинный веб-сайт финансового учреждения. Это сбивает с толку владельцев зараженных Shylock компьютеров и дает Ответчикам возможность осуществлять свои атаки по фальсификации веб-сайтов. Это также почти полностью исключает возможность выявления атак пользователями.

44. В рамках еще более изощренной схемы Shylock поддерживает встроенный сервер виртуальной сетевой консоли (VNC), обладающий способностью подключаться к удаленному серверу. Эта функция позволяет Ответчикам получать прямой доступ к зараженному компьютеру по Интернету, обходя ограничения трансляции сетевых номеров и брандмауэра на входящих соединениях. С этого узла оператор бот-сети может подключать компьютер пользователя к банку и использовать данные входа в систему, ранее похищенные у пользователя, для кражи средств с его банковских счетов.

45. Кроме того, Shylock может вести видеозапись действий пользователя в Интернете. Эта функция может использоваться для хищения конфиденциальной информации, такой как балансы счетов, либо для перехвата аутентификационной информации. Способность вести видеозапись позволяет злоумышленнику отслеживать фрагменты всего интернет-сеанса пользователя при обращении к целевому веб-сайту. Эти сведения могут быть полезны злоумышленнику, чтобы лучше понять принцип действия онлайнового банковского приложения. Встраиваемый модуль видеозахвата обычно

загружается с командно-контрольной инфраструктуры Shylock.

46. Shylock специально предназначен для того, чтобы позволить Ответчикам осуществлять эту противозаконную деятельность, не давая обнаружить следы мошенничества пользователю, компании Microsoft, финансовым учреждениям или другим пострадавшим веб-сайтам до тех пор, пока пользователь или владельцы этих веб-сайтов в силу упущенного времени уже не смогут восстановить контроль над средствами или похищенной информацией. Например, во избежание предупреждения пользователя об активности его компьютера, осуществляемой дистанционно, Shylock посылает команду на отключение всех звуковых сигналов (например, гудков или щелчков), которые в противном случае могли бы предупредить пользователя о дистанционном контроле его компьютера. Многие аспекты сбора информации и проведения атак могут быть автоматизированы оператором бот-се, так чтобы бот-код, действующий на каждом индивидуальном компьютере пользователя, мог способствовать совершению кражи автономно.

Ответчики используют зараженные компьютеры для совершения атак на другие компьютеры в Интернете

47. Ответчики разработали встраиваемые модули, позволяющие им совершать атаки на другие компьютеры в Интернете. Встраиваемый модуль MessengerSpread, например, позволяет Ответчикам заражать другие компьютеры в Интернете с помощью программ мгновенной передачи сообщений. Встраиваемый модуль RAT (технология удаленного доступа) Ответчиков, кроме того, дает им возможность атаковать другие компьютеры в локальной сети зараженного компьютера. Ответчики раздают эти встраиваемые модули на зараженные пользовательские компьютеры с помощью доменов Plug-in Shylock, которые перечислены в Приложении A.

Вред, причиняемый бот-сетями Shylock

48. Само заражение вредоносными программами Shylock вредит компании Microsoft и ее клиентам тем, что наносит вред компьютерам пользователей и установленному на них программному обеспечению, лицензированному компанией

Microsoft. При заражении компьютера пользователя вредоносные программы Shylock изменяют операционную систему компьютера на самых глубинных и наиболее чувствительных ее уровнях. Кроме того, они вносят фундаментальные изменения на уровне системного реестра Windows. Пользователи Microsoft, чьи компьютеры заражены вредоносными программными средствами, страдают от этих изменений Windows, которые нарушают нормальные и утвержденные настройки и функции операционной системы пользователя, дестабилизируют ее и принудительно втягивают компьютеры пользователей в бот-сеть.

49. После заражения компьютера ОС Windows и браузер Internet Explorer на этом компьютере перестают нормально функционировать и трансформируются в орудия обмана и хищения. Но Windows и Internet Explorer по-прежнему являются торговыми марками компании Microsoft. Пользователи, сталкивающиеся с ухудшением работы продуктов Microsoft, могут отнести такое ухудшение работы на счет Microsoft, что является серьезным ударом по имиджу брендов и торговых марок Microsoft и доброму отношению к ним клиентов. Даже те пользователи, которые в конечном итоге убеждаются в том, что их компьютеры заражены вредоносными программами, могут прийти к ошибочному выводу, что заражение произошло из-за уязвимостей продуктов Microsoft, поскольку многим из пользователей неизвестно, что они стали жертвами атак Ответчиков.

50. Кроме того, являясь провайдером продуктов Windows и Internet Explorer, компания Microsoft направляет значительные компьютерные и людские ресурсы на борьбу с заражением вредоносными программами бот-сети Shylock, помогая пользователям определить, заражены ли их компьютеры, и очищая зараженные компьютеры. Эти усилия компании Microsoft влекут за собой существенные финансовые расходы, следовательно, бот-сеть Shylock и ее вредоносные программы наносят ощутимый экономический урон компании Microsoft.

51. Бот-сети Shylock и связанные с ними вредоносные программы наносят вред многочисленным пользователям, а также финансовым учреждениям, чьи интересы представляет FS-ISAC, равно как и самому FS-ISAC. Как и компания Microsoft, FS-ISAC

направляет существенные ресурсы на расследование и ликвидацию ущерба, вызванного бот-сетями Shylock. Кроме того, торговые марки, бренды и торговые названия учреждений FS-ISAC используются для обмана владельцев зараженных Shylock компьютеров с целью получения Ответчиками данных доступа в систему и другой личной идентифицирующей информации. Учреждения FS-ISAC, кроме того, несут прямые финансовые потери в результате противозаконной деятельности Ответчиков. Ответчики и бот-сети Shylock нанесли учреждениям-членам FS-ISAC многомиллионный ущерб.

Ответчики действуют сообща в рамках совместной операции по созданию, контролю, обслуживанию и эксплуатации бот-сетей Shylock

52. Бот-сети Shylock образуют семейство взаимосвязанных бот-сетей, известных под общим названием «вредоносные программы Shylock». Вредоносные программы Shylock впервые обнаружили себя в 2011 году. С течение времени они эволюционировали, стали более совершенными и пополнились дополнительными функциями, разработанными для противодействия попыткам анализа и вывода из строя бот-сетей.

53. Истцы располагают информацией, убеждены и на этом основании утверждают, что общий код и характеристики бот-сетей Shylock и свидетельства, касающиеся конкретных действий Ответчиков, демонстрируют, что Ответчики, действуя согласованно друг с другом, контролируют бот-сети Shylock. Согласно имеющейся информации и существующему убеждению, вредоносные программы Shylock, которые Ответчики устанавливают на компьютерах пользователей, обладают общим кодом и характеристиками, и в процессе развития с течением времени приобрели ряд сходных общих для всех них свойств. Бот-сети Shylock используют сходные конфигурационные файлы бот-сетей семейства Zeus. Кроме того, все конфигурационные файлы Shylock имеют аналогичные структуры и используют аналогичные команды для управления и контроля пользовательских компьютеров, зараженных Shylock. Помимо этого, Ответчики используют одни и те же домены, сервера имен, IP-адреса и номера телефонов, которые входят в командно-контрольную инфраструктуру Shylock.

54. Каждый из Ответчиков принимал участие в деятельности схемы Shylock в следующих аспектах: (1) разработка исполняемых файлов Shylock, конфигурационных файлов и встраиваемых модулей для контроля пользовательских компьютеров; (2) развертывание бот-сетей Shylock под одним именем бот-сети; (3) создание и обслуживание командно-контрольной инфраструктуры Shylock, состоящей из серверов, подключенных к Интернету и осуществляющих связь с зараженными пользовательскими компьютерами; (4) использование одного или нескольких средств для заражения пользовательских компьютеров с помощью Shylock; (5) использование зараженных Shylock компьютеров по всему миру для хищения секретной идентификационной и финансово-бухгалтерской информации; (6) использование ботов Shylock для хищения денег непосредственно с финансовых счетов ничего не подозревающих пользователей по всему миру; (7) повреждение принадлежащего компании Microsoft и лицензированного ею программного обеспечения, включая Windows и Internet Explorer, путем нарушения работы этих программ и превращения их в орудия совершения преступлений; (8) эксплуатация известных брендов и торговых марок Microsoft для введения в заблуждение пользователей и, как следствие, причинения серьезного ущерба бренду, торговым маркам, репутации и авторитета компании Microsoft; (9) использование зараженных Shylock компьютеров для рассылки подложных мгновенных сообщений; а также (10) использование зараженных Shylock компьютеров для запуска атак распределенного отказа в обслуживании против финансовых и других учреждений..

The Shylock Racketeering Enterprise

55. Истцы располагают информацией, имеют понимание и в этой связи утверждают, что Ответчики сотрудничают с целью разработки, улучшения и поддержки бот-сетей «Шейлок», а также инфраструктуры управления и контроля бот-сетей «Шейлок». По имеющейся у Истцов информации, Ответчики представляют собой группу лиц, связанных между собой общей целью вхождения в контакт – в ходе длящегося поведения и в рамках постоянно действующей организации – с разного рода соучастниками, функционирующими в качестве постоянно действующих

организационных единиц. У организации Ответчиков имеется цель, осуществление которой достигается посредством отношений всех ее участников, а срок ее существования позволяет ее участникам придерживаться намеченной цели. По имеющейся у Истцов информации, Ответчики Джон Доу 1-8 сговорились о создании организации без статуса юридического лица (associated in fact enterprise) (в дальнейшем Shylock Racketeering Enterprise), и создали такую организацию, с общей целью по разработке и управлению глобальной бот-сетью, крадущей учетные данные, как это подробно изложено в настоящем документе.

56. Shylock Racketeering Enterprise существует по меньшей мере с сентября 2011 года, когда Ответчиками была открыто создана единая, консолидированная глобальная бот-сеть, крадущая учетные данные. К Shylock Racketeering Enterprise присоединились и другие Ответчики.

57. Начиная с указанного времени, Shylock Racketeering Enterprise непрерывно и эффективно осуществляет свою цель, разработав крадущую учетные данные глобальную бот-сеть и управляя этой бот-сетью, и будет продолжать осуществлять эту цель при отсутствии средства судебной защиты, запрашиваемого Истцами.

58. Цель создания Shylock Racketeering Enterprise, а также отношений между Ответчиками была установлена в связи с: (1) появлением бот-сетей «Шейлок»; (2) последующим развитием и функционированием бот-сетей «Шейлок»; и (3) существованием для удовлетворения общих финансовых интересов Ответчиков согласованных между собой функциональных ролей Ответчиков, связанных с эксплуатацией, техническим обслуживанием и прибылью от бот-сетей «Шейлок».

59. По имеющейся у Истцов информации, Ответчики по предварительному сговору, умышленно и с намерением противоправно завладеть чужим имуществом, проводили и участвовали в операциях Shylock Racketeering Enterprise с применением постоянной схемы захвата собственности других лиц, как это подробно изложено в настоящем документе. Каждое предикатное деяние связано и осуществлено для удовлетворения общей незаконной цели, преследуемой каждым из участников Shylock

Racketeering Enterprise. Эти деяния продолжают осуществляться и продолжать осуществляться до тех пор, пока суд не удовлетворит ходатайство Истцов о наложении временного судебного запрета и применении других средств судебной защиты.

60. По имеющейся у Истцов информации, Ответчики по предварительному сговору, умышленно и с намерением противоправно завладеть чужим имуществом незаконно ввели в оборот тысячи средств несанкционированного доступа в виде украденных паролей, номеров банковских счетов и другой учетной информации через разработанные и управляемые Ответчиками бот-сети «Шейлок».

61. Как подробно изложено в настоящем документе, Ответчики использовали бот-сети «Шейлок» для кражи, перехвата и получения информации о средствах несанкционированного доступа от десятков тысяч лиц, использующих подложные веб-страницы, а потом использовали эти полученные обманным путем средства несанкционированного доступа для кражи миллионов долларов со счетов физических лиц.

62. По имеющейся у Истцов информации, Ответчики также по предварительному сговору, умышленно и с намерением противоправно завладеть чужим имуществом завладели тысячами таких средств несанкционированного доступа, полученных обманным путем, как это описано в настоящем документе.

63. По имеющейся у Истцов информации, Ответчики также по предварительному сговору, умышленно и с намерением противоправно завладеть чужим имуществом осуществили транзакции при помощи средств несанкционированного доступа, использовав миллионы долларов с банковских счетов физических лиц в качестве средства оплаты.

64. По имеющейся у Истцов информации, Ответчики по предварительному сговору реализовали схему обмана десятков финансовых учреждений, когда участники Shylock Racketeering Enterprise обманным путем представляли себя в качестве клиентов банков, получали доступ к средствам на клиентских счетах и выводили с них средства.

65. Каждое из вышеуказанных незаконных действий было осуществлено с использованием межштатных автоматизированных расчетных палат и/или межштатных

и/или зарубежных телефонных линий, как это описано в настоящем документе, и, следовательно, отрицательно сказалось как на торговле на уровне штатов, так и на внешней торговле.

ПЕРВОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Нарушение закона «О компьютерном мошенничестве и злоупотреблении», раздел 18, § 1030

66. Истцы включают в настоящий раздел путем ссылки все утверждения, приведенные в пунктах с 1 по 65 выше.

67. Ответчики по предварительному сговору, умышленно и с намерением противоправно завладеть чужим имуществом осуществляли несанкционированный доступ к защищенным компьютерам и сознательно вызывали передачу программы, информации, кода и команд, наносящих ущерб защищенным компьютерам, установленному на них программному обеспечению, и Microsoft.

68. Поведение Ответчиков задействовало средства информационного взаимодействия между штатами и/или внешние средств информационного взаимодействия.

69. Поведение Ответчиков привело к ущербу для каждого из Истцов в общей сумме не менее 5 000 долл. США в течение одного года.

70. Истцы добиваются наложения судебного запрета и возмещения фактических и штрафных убытков на основании положений раздела 18, § 1030(g) в размере, определенном в ходе судебного разбирательства.

71. Действиями Ответчиков Истцам был нанесен и продолжает наноситься непоправимый вред, в отношении которого не существует надлежащего средства правовой защиты и нанесение которого будет продолжаться до тех пор, пока на действия Ответчиков не будет наложен запрет.

ВТОРОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Нарушение закона «О защите электронных систем связи», раздел 18, § 2701

72. Истцы включают в настоящий раздел путем ссылки все утверждения,

приведенные в пунктах с 1 по 65 выше.

73. Операционная система Microsoft Windows, программное обеспечение Internet Explorer, компьютеры клиентов Microsoft, использующие такое программное обеспечение, являются объектами, через которые услуги электронной связи предоставляются пользователям и клиентам Microsoft.

74. Ответчики сознательно и преднамеренно осуществляли доступ в операционную систему Windows, программное обеспечение Internet Explorer и компьютеры с таким установленным программным обеспечением, не имея на то необходимого разрешения или сверх границ, установленных разрешением, предоставленным Microsoft или любой другой стороной.

75. Путем такого несанкционированного доступа Ответчики осуществляли перехват, имели доступ, получали и изменяли и/или препятствовали законному, санкционированному доступу к информации, передаваемой электронным способом средствами операционной системы Microsoft Windows и программного обеспечения Internet Explorer и компьютерами с таким установленным программным обеспечением.

76. Истцы добиваются наложения судебного запрета и возмещения фактических и штрафных убытков в размере, определенном в ходе судебного разбирательства.

77. Действиями Ответчиков Истцам был нанесен и продолжает наноситься непоправимый вред, в отношении которого не существует надлежащего средства правовой защиты и нанесение которого будет продолжаться до тех пор, пока на действия Ответчиков не будет наложен запрет.

ТРЕТЬЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Нарушение товарного знака, закон Лэнхема - раздел 15, § 1114 *и далее.*

78. Истцы включают в настоящий раздел путем ссылки все утверждения, приведенные в пунктах с 1 по 65 выше.

79. Ответчики использовали товарные знаки Microsoft и организаций FS-ISAC в торговых операциях между штатами.

80. Бот-сети «Шейлок» генерируют и используют незаконные копии товарных

знаков Microsoft в поддельных и незаконных версиях операционной системы Windows и программного обеспечения Internet Explorer, в том числе с помощью программного обеспечения, работающего через инфраструктуру управления и контроля бот-сетей «Шейлок». Бот-сети «Шейлок» также генерируют и используют незаконные копии товарных знаков организаций FS-ISAC. Такие действия Ответчиков способны вызвать путаницу, ошибки или ввести в заблуждение относительно происхождения, финансирования или одобрения поддельных и незаконных версий операционной системы Windows и программного обеспечения Internet Explorer.

81. Ответчики несут ответственность перед Истцами за свои неправомерные действия, осуществленные в нарушение положений закона Лэнхема.

82. Истцы добиваются наложения судебного запрета и возмещения фактических и штрафных убытков в размере, определенном в ходе судебного разбирательства.

83. Действиями Ответчиков Истцам был нанесен и продолжает наноситься непоправимый вред, в отношении которого у них нет надлежащего средства правовой защиты и нанесение которого будет продолжаться до тех пор, пока на действия Ответчиков не будет наложен запрет.

84. Противоправное и несанкционированное использование Ответчиками товарных знаков Microsoft и организаций FS-ISAC в целях вывода на рынок или продажи товаров и услуг представляет собой нарушение товарного знака в соответствии с разделом 15, § 1114 и далее.

ЧЕТВЕРТОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Неправильное обозначение места происхождения товара, закон Лэнхема - раздел 15, § 1125 (a)

85. Истцы включают в настоящий раздел путем ссылки все утверждения, приведенные в пунктах с 1 по 65 выше.

86. Товарными знаками Microsoft и организаций-участниц FS-ISAC являются отличительные знаки, связанные с Microsoft и организациями-участницами FS-ISAC и служащие единственной целью отождествления характера их деловой активности,

продуктов и услуг.

87. Ответчики незаконно использовали товарные знаки Microsoft и организаций-участниц FS-ISAC. Таким образом, действия Ответчиков создают неправильное обозначение места происхождения услуг Microsoft и организаций-участниц FS-ISAC и способны вызвать путаницу, ошибки или ввести в заблуждение.

88. Ответчики несут ответственность перед Истцами за свои неправомерные действия, осуществленные в нарушение закона Лэнхема, раздел 15, § 1125(a).

89. Истцы добиваются наложения судебного запрета и возмещения фактических и штрафных убытков в размере, определенном в ходе судебного разбирательства.

90. Действиями Ответчиков Истцам был нанесен и продолжает наноситься непоправимый вред, в отношении которого у них нет надлежащего средства правовой защиты и нанесение которого будет продолжаться до тех пор, пока на действия Ответчиков не будет наложен запрет.

ПЯТОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Размывание товарного знака, закон Лэнхема - раздел 15, § 1125(c)

91. Истцы включают в настоящий раздел путем ссылки все утверждения, приведенные в пунктах с 1 по 65 выше.

92. Товарными знаками Microsoft и организаций-участниц FS-ISAC являются общеизвестные знаки, связанные с Microsoft и организациями-участницами FS-ISAC и служащие единственной целью отождествления характера их деловой активности, продуктов и услуг.

93. Ответчики незаконно использовали товарные знаки Microsoft и организаций-участниц FS-ISAC. Такие действия Ответчиков способны вызвать размывание товарных знаков Истцов, поскольку порочат репутацию владельцев товарных знаков.

94. Истцы добиваются наложения судебного запрета и возмещения фактических и штрафных убытков в размере, определенном в ходе судебного разбирательства.

95. Действиями Ответчиков Истцам был нанесен и продолжает наноситься

непоправимый вред, в отношении которого у них нет надлежащего средства правовой защиты и нанесение которого будет продолжаться до тех пор, пока на действия Ответчиков не будет наложен запрет.

ШЕСТОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ
Нарушение закона «О вымогательстве и преступных организациях» (RICO) - раздел 18, § 1962(c) (Microsoft)

96. Microsoft повторно ссылается на все утверждения, приведенные в пунктах с 1 по 65 выше.

97. Начиная с сентября 2011 года, во время этой даты и после нее и на всем протяжении периода подачи настоящей Жалобы, Ответчики Джон Доу 1-8 были и остаются участниками Shylock Racketeering Enterprise и ведут дела этой организации с применением постоянной схемы захвата собственности других лиц, при этом такое поведение и действия оказывают влияние как на торговлю на уровне штатов, так и на внешнюю торговлю. В разные моменты времени после сентября 2011 года и на всем протяжении периода подачи настоящей Жалобы, Ответчики Джон Доу 2-8 стали участниками Shylock Racketeering Enterprise и также вели и участвовали в делах этой организации с применением постоянной схемы захвата собственности других лиц, которая оказывает влияние как на торговлю на уровне штатов, так и на внешнюю торговлю. Ответчики занимаются организованным преступным захватом собственности других лиц, осуществляя тысячи предикатных преступлений – мошенничество и сопутствующая деятельность, связанная с использованием средств доступа (раздел 18, § 1029), мошенничество с использованием телефонной линии (раздел 18, § 1343) и мошенничество в банковской сфере (раздел 18, § 1344).

98. Как указано выше, участники Shylock Racketeering Enterprise имеют общую цель по разработке и управлению глобальной бот-сетью, крадущей учетные данные.

99. Ответчики по предварительному сговору, умышленно и с намерением противоправно завладеть чужим имуществом незаконно ввели в оборот тысячи средств несанкционированного доступа в виде украденных паролей, номеров банковских счетов и

другой учетной информации через разработанные и управляемые Ответчиками бот-сети «Шейлок». Как подробно изложено выше, Ответчики использовали бот-сети «Шейлок» для кражи, перехвата и получения информации о средствах несанкционированного доступа от тысяч лиц, использующих подложные веб-страницы, а потом использовали эти полученные обманным путем средства несанкционированного доступа для кражи многих миллионов долларов со счетов физических лиц – все это в нарушение положений раздела 18, § 1029(a)(2).

100. В нарушение положений раздела 18, § 1029(a)(3), Ответчики также по предварительному сговору, умышленно и с намерением противоправно завладеть чужим имуществом завладели тысячами средств несанкционированного доступа, полученных обманным путем, как это описано в настоящем документе.

101. В нарушение положений раздела 18, § 1029(a)(7), Ответчики также по предварительному сговору, умышленно и с намерением противоправно завладеть чужим имуществом осуществили транзакции при помощи средств несанкционированного доступа, использовав миллионы долларов с банковских счетов физических лиц в качестве средства оплаты.

102. Как подробно изложено выше, в нарушение положений раздела 18, § 1344, Ответчики реализовали схему обмана десятков финансовых учреждений, когда участники Shylock Racketeering Enterprise обманным путем представляли себя в качестве клиентов банков, получали доступ к средствам на клиентских счетах и выводили с них средства.

103. Каждое из описанных выше нарушений положений раздела 18, § 1029(a) и раздела 18, § 1344, было осуществлено с использованием средств межсетевого информационного обмена, «осуществляемого по телефонной линии ... и затрагивающим межтатную и внешнюю торговлю» в нарушение положений раздела 18, § 1343.

104. Поведение Ответчиков нанесло и продолжает наносить прямой ущерб Microsoft. Microsoft бы не понесла убытков при отсутствии такой организованной деятельности по преступному захвату собственности других лиц.

105. Microsoft добивается наложения судебного запрета и возмещения

фактических и штрафных убытков в размере, определенном в ходе судебного разбирательства.

СЕДЬМОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Нормы общего права в отношении посягательства на движимое имущество

106. Истцы включают посредством ссылки все обвинения, изложенные в пунктах 1-65 выше.

107. Ответчики использовали компьютер и/или компьютерную сеть без разрешения с намерением нанести физическое повреждение имуществу других лиц.

108. Ответчики без разрешения использовали компьютер и/или компьютерную сеть с намерением посягать на компьютеры и компьютерные сети организаций-членов FS-ISAC.

109. Действия Ответчиков при управлении бот-сетями «Шейлок» привели к неавторизованному доступу к операционной системе Windows компании Microsoft, программе Internet Explorer и компьютерам, на которых запущена эта программа, а также к неавторизованному вторжению в эти компьютеры и краже информации, данных учетных записей и денежных средств.

110. Ответчики делали это намеренно, и такие действия были незаконными и неразрешенными.

111. Действия Ответчиков нанесли ущерб компании Microsoft, FS-ISAC и организациям-членам FS-ISAC и вступили в конфликт с владельческим правом компании Microsoft на ее программное обеспечение, а также с владельческим правом организаций-членов FS-ISAC на их соответствующие компьютеры и компьютерные сети.

112. Истцы требуют вынесения судебного запрета, возмещения убытков и возмещения убытков в виде наказания в размере, установленном судом.

113. Как прямой результат действий Ответчиков Истцы и Организации-члены FS-ISAC понесли и продолжают нести необратимый ущерб, для которого закон не предусматривает адекватного возмещения и который будет сохраняться до тех пор, пока не будут запрещены действия Ответчиков.

ВОСЬМОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Неосновательное обогащение

114. Истцы включают посредством ссылки все обвинения, изложенные в пунктах 1-65 выше.

115. Действия Ответчиков, ставшие предметом данного иска, представляют собой неосновательное обогащение Ответчиков за счет компании Microsoft и организаций-членов FS-ISAC в нарушение общего права. Ответчики использовали, без разрешения и лицензии, программное обеспечение, принадлежащее компании Microsoft, для осуществления противоправных действий в интересах Ответчиков.

116. Ответчики неосновательно обогатились в результате неразрешенного и нелицензированного использования интеллектуальной собственности компании Microsoft.

117. По имеющейся информации и убеждению, Ответчики понимали и знали, какую выгоду они получили в результате неразрешенного и нелицензированного использования интеллектуальной собственности компании Microsoft.

118. Удержание Ответчиками прибыли, полученной в результате их противоправного действия, было бы несправедливым.

119. Истцы требуют вынесения судебного запрета, возмещения убытков и возмещения убытков в виде наказания в размере, установленном судом, включая возвращение доходов Ответчиков, полученных незаконным путем.

120. Как прямой результат действий Ответчиков Истцы и Организации-члены FS-ISAC понесли и продолжают нести необратимый ущерб, для которого закон не предусматривает адекватного возмещения и который будет сохраняться до тех пор, пока не будут запрещены действия Ответчиков.

ДЕВЯТОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Перевод

121. Истцы включают посредством ссылки все обвинения, изложенные в пунктах 1-65 выше.

122. Компании Microsoft принадлежат все права, право собственности и доля

собственности на программное обеспечение Windows и Internet Explorer. Компания Microsoft выдает лицензии на свое программное обеспечение конечным пользователям. Ответчики создали препятствия, незаконно и без разрешения, и лишили компанию Microsoft прав владения программным обеспечением Windows и Internet Explorer.

123. Ответчики без разрешения использовали компьютер и/или компьютерную сеть с намерением удалить, отключить или иным способом заблокировать компьютерные данные, компьютерные программы и программное обеспечение, установленные на компьютере или в компьютерной сети.

124. Ответчики без разрешения использовали компьютер и/или компьютерную сеть с намерением нарушить функционирование компьютера.

125. Ответчики перевели денежные средства организаций-членов FS-ISAC путем снятия средств со счетов клиентов, используя украденные банковские данные.

126. Истцы требуют вынесения судебного запрета, возмещения убытков и возмещения убытков в виде наказания в размере, установленном судом, включая возвращение доходов Ответчиков, полученных незаконным путем.

127. Как прямой результат действий Ответчиков Истцы и Организации-члены FS-ISAC понесли и продолжают нести необратимый ущерб, для которого закон не предусматривает адекватного возмещения и который будет сохраняться до тех пор, пока не будут запрещены действия Ответчиков.

ХОДАТАЙСТВО О ПРЕДОСТАВЛЕНИИ СУДЕБНОЙ ЗАЩИТЫ

В СВЯЗИ С ЧЕМ, Истцы ходатайствуют о том, чтобы Суд:

1. вынес решение в пользу Истцов против Ответчиков.

2. признал действия Ответчиков намеренными, мошенническими, умышленными и угнетающими.

3. вынес предварительное бессрочное судебное предписание, запрещающее Ответчикам и их руководителям, директорам, начальникам, агентам, служащим, сотрудникам, правопреемникам и цессионариям, а также всем физическим и юридическим лицам, находящимся активном взаимодействии и сотрудничестве с ними, участвовать в

любой деятельности, ставшей предметом данного иска, или наносить любой ущерб, ставший предметом данного иска, а также помогать, способствовать и пособничать другому физическому или юридическому лицу в участии или осуществлении деятельности или причинении ущерба, ставших предметом данного иска.

4. вынес предварительное бессрочное судебное предписание, предоставляющее компании Microsoft контроль над доменами, IP-адресами и номерами телефонов, использовавшимися Ответчиками, и запрещающее Ответчикам использовать такие инструменты.

5. вынес решение о возмещении Истцам фактического ущерба, нанесенного Ответчиками, достаточного для компенсации ущерба, нанесенного Истцам действиями Ответчиков, ставшими предметом данного иска, а также ущерба, ставшего предметом данного иска, включая проценты и издержки в размере, установленном судом.

6. вынес решение о возвращении Ответчиками незаконно присвоенной прибыли.

7. вынес решение о расширенных, карательных и фактических убытках, определяемых особыми обстоятельствами дела, в установленном судом размере.

8. вынес решение о возмещении судебных издержек и расходов на адвокатов.

9. вынес решение относительно других средств судебной защиты, которые Суд посчитает справедливыми и обоснованными.

Дата: 30 июня 2014

Требование подано:

ORRICK, HERRINGTON & SUTCLIFFE LLP

_____

LAUREN J. PARKER
Лицензия № 77018 Коллегии адвокатов штата Виргиния
Адвокаты истцов: Microsoft Corp. и FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Телефон: (202) 339-8400
Факс: (202) 339-8500
lparker@orrick.com

От группы адвокатов:

GABRIEL M. RAMSEY (подано ходатайство о разрешении на одноразовое представительство)
JACOB M. HEATH (подано ходатайство о разрешении на одноразовое представительство)
ROBERT L. URIARTE (подано ходатайство о разрешении на одноразовое представительство)
Адвокаты истцов: Microsoft Corp. и FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Телефон: (650) 614-7400
Факс: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com
ruriarte@orrick.com

ТРЕБОВАНИЕ О РАССМОТРЕНИИ ДЕЛА СУДОМ присяжных

Истцы с почтением просят рассмотреть дело судом присяжных по всем пунктам, подлежащим такому рассмотрению в соответствии со статьей 38 Федеральных правил гражданского судопроизводства.

Дата: 30 июня 2014

Требование подано:

ORRICK, HERRINGTON & SUTCLIFFE LLP

LAUREN J. PARKER
Лицензия № 77018 Коллегии адвокатов штата Виргиния
Адвокаты истцов: Microsoft Corp. и FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
Телефон: (202) 339-8400
Факс: (202) 339-8500
lparker@orrick.com

От группы адвокатов:

GABRIEL M. RAMSEY (подано ходатайство о разрешении на одноразовое представительство)
JACOB M. HEATH (подано ходатайство о разрешении на одноразовое представительство)
ROBERT L. URIARTE (подано ходатайство о разрешении на одноразовое представительство)
Адвокаты истцов: Microsoft Corp. и FS-ISAC, Inc.
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Телефон: (650) 614-7400
Факс: (650) 614-7401
gramsey@orrick.com
jheath@orrick.com
ruriarte@orrick.com